Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - **3Com 3CDaemon Multiple Remote Vulnerabilities (Updated)**
  - aeNovo Information Disclosure
  - GoodTech Systems Telnet Server for Windows NT/2000/XP/2003 Remote Buffer Overflow
  - Ipswitch IMail Server IMAP EXAMINE Command Remote Buffer Overflow
  - Microsoft Exchange Server Nested Subfolders Remote Denial of Service
  - Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote Denial of Service
  - **Microsoft Windows SMB Buffer Overflow (Updated)**
  - **Microsoft Internet Explorer Vulnerabilities (Updated)**
  - PlatinumFTPServer Malformed User Name Connection Remote Denial of Service
  - PY Software Active Webcam Webserver Remote Denials of Service & Information Disclosure
  - **SafeNet Sentinel License Manager Remote Buffer Overflow (Updated)**
  - Symantec AntiVirus SMB Scan Detection Bypass
  - Techland XPand Rally Remote Format String
  - Yahoo! Messenger Custom Message Buffer Overflow
- UNIX / Linux Operating Systems
  - **Black List Daemon select() Remote Buffer Overflow (Updated)**
  - Frank McIngvale LuxMan Buffer Overflow
  - Freeciv Remote Denial of Service
  - **Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow (Updated)**
  - **GNU CPIO Archiver Insecure File Creation (Updated)**
  - **GNU Xpdf Buffer Overflow in doImage() (Updated)**
  - Grip CDDB Query Buffer Overflow
  - HP Tru64 Message Queue Denial of Service
  - **Hiroyuki Yamamoto Sylpheed Mail Client Remote Buffer Overflow (Updated)**
  - **ISC DHCPD Package Remote Format String (Updated)**
  - **LibEXIF Library EXIF Tag Structure Validation (Updated)**
  - Marc Lehmann rxvt-unicode 'command.c' Remote Buffer Overflow
  - **Michael Kohn Ringtone Tools parse_emelody() Buffer Overflow (Updated)**
  - **Multiple Vendors Libdbi-perl Insecure Temporary File Creation (Updated)**
  - Multiple Vendors Perl 'rmtree()' Function Elevated Privileges
  - **Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability (Updated)**
  - Multiple Vendors KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Local Buffer Overflows & Information Disclosure (Updated)**
  - Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service
  - Multiple Vendors Linux Kernel SYS_EPoll_Wait Elevated Privileges
  - Multiple Vendor Antivirus Products Malformed ZIP Archive Scan Evasion Bypass
  - **Multiple Vendors LibXPM Bitmap_unit Integer Overflow (Updated)**
  - NewsScript Access Validation
  - **OpenBSD TCP Timestamp Remote Denial of Service (Updated)**
  - OpenSLP Multiple Buffer Overflows
  - PaFileDB Multiple Cross-Site Scripting
  - PaFileDB 'viewall.php' and 'category.php' Input Validation
  - PaFileDB Installation Path Disclosure
  - **Rob Flynn Gaim Multiple Remote Denials of Service (Updated)**
  - **Squid Proxy FQDN Remote Denial of Service (Updated)**
  - **SquirrelMail Remote Code Execution (Updated)**
  - **SquirrelMail S/MIME Plug-in Remote Command Execution (Updated)**
  - **The PaX Team PaX Undisclosed Arbitrary Code Execution (Updated)**
  - Wine Insecure File Creation

Multiple Operating Systems

- All Enthusiast PhotoPost PHP Pro Multiple Vulnerabilities
- ApplyYourself i-Class Information Disclosure Vulnerability
- Bernd Ritter HolaCMS Lets Remote Users Modify Files
- Bösch SimpGB "quote" SQL Injection Vulnerability
- **Cisco ACNS Denial of Service Vulnerabilities (Updated)**
- **Computer Associates License Remote Code Execution Vulnerability (Updated)**
- **Ethereal Buffer Overflow (Updated)**
  Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities
- **GNU Gaim Denial of Service Vulnerability (Updated)**
- GNU WF-Sections Input Validation Vulnerability
- GNU Xoops Avatar Upload File Extension Vulnerability
- GNU YaBB Cross-Site Scripting Vulnerability
- Hensel Hartmann VoteBox Arbitrary Code Execution Vulnerability
- Hitachi Cosminexus Server Component Container Tomcat Denial of Service
- IBM WebSphere Commerce Private Information Disclosure

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
3Com 3CDaemon 2.0 revision 10	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when a remote malicious user submits a specially crafted FTP username, which could lead to the execution of arbitrary code; a buffer overflow vulnerability exists in several FTP commands, including cd, send, ls, put, delete, rename, rmdir, literal, stat, and cwd, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability exists when a malicious user submits an FTP user command with format string characters; a format string vulnerability exists in the cd, delete, rename, rmdir, literal, stat, and cwd [and others] commands, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability exists when a malicious user connects to the TFTP service and requests an MS-DOS device name; a vulnerability exists when the directory to an MS-DOS device name or a filename is changed, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. **Another exploit script has been published.**	3Com 3CDaemon Multiple Remote Vulnerabilities CAN-2005-0275 CAN-2005-0276 CAN-2005-0277 CAN-2005-0278	Low/Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	[I.T.S] Security Research Team Advisory, January 4, 2005 Security Focus, 12155, February 19, 2005 **Security Focus, 12155, March 15, 2005**

FutureStore Technologies Ltd aeNovo	A vulnerability has been reported in the default configuration because the 'dbase/aeNovo1.mdb' database file can be accessed directly, which could let a remote malicious user obtain sensitive information, including the administrative password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	aeNovo Information Disclosure	Medium	Secunia Advisory, SA14580, March 14, 2005
GoodTech Telnet Server for Windows NT/2000/XP/2003 4.0, 5.0	A buffer overflow vulnerability has been reported due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. Update available at: http://www.goodtechsys.com A Proof of Concept exploit script has been published.	GoodTech Systems Telnet Server for Windows NT/2000/XP/2003 Remote Buffer Overflow	High	BugTraq, 393295March 15, 2005
Ipswitch IMail 5.0, 5.0.5-5.0.8, 6.0-6.0.6, 6.1-6.4, 7.0.1-7.0.7, 7.1, 7.12, 8.0.3, 8.0.5, 8.1, 8.13, Ipswitch Collaboration Suite	A buffer overflow vulnerability has been reported in the EXAMINE command in the IMAP daemon due to improper processing of user-supplied parameters, which could let a remote malicious user execute arbitrary code with administrator privileges. Hotfix available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/IM815HF1.exe Currently we are not aware of any exploits for this vulnerability.	Ipswitch IMail Server IMAP EXAMINE Command Remote Buffer Overflow CAN-2005-0707	High	iDEFENSE Security Advisory, March 10, 2005
Microsoft Exchange Server 2003, SP1	A remote Denial of Service vulnerability has been reported due to a stack overflow when deleting or moving a folder that contains multiple nested subfolders. Hotfix available at: http://support.microsoft.com/default.aspx?scid=fh;[LN];CNTACTMS There is no exploit code required.	Microsoft Exchange Server Nested Subfolders Remote Denial of Service CAN-2005-0738	Low	Secunia Advisory: SA14543, March 9, 2005
Microsoft Internet Explorer 6.0 SP2 Microsoft Internet Explorer 6.0 SP1 Microsoft Internet Explorer 6.0	A remote Denial of Service vulnerability has been reported due to a buffer overflow in 'mshtml.dll' CSS handling. No workaround or patch available at time of publishing. An exploit script has been published.	Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote Denial of Service CAN-2004-0842	Low	Securiteam, March 9, 2005
Microsoft Windows 2000 SP3 & SP4, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A buffer overflow vulnerability exists when handling Server Message Block (SMB) traffic, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx **Microsoft Windows NT 4.0 has also been found vulnerable to the issue; however, this platform is no longer publicly supported by Microsoft. A patch is available for customers that have an active end-of-life support agreement including extended Windows NT 4.0 support. Information regarding the end-of-life support agreement can be found at the following location: http://www.microsoft.com/presspass/features/2004/dec04/12-03NTSupport.asp** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows SMB Buffer Overflow CAN-2005-0045	High	Microsoft Security Bulletin, MS05-011, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#652537 **Security Focus, 12484, March 9, 2005**

Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1 (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	Multiple vulnerabilities exist: a vulnerability exists due to insufficient validation of drag and drop events from the Internet zone to local resources, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to the way certain encoded URLs are parsed, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the validation of URLs in CDF (Channel Definition Format) files, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to an input validation error in the 'createControlRange()' javascript function, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient cross-zone restrictions; a vulnerability exists due to the way web sites are handled inside the 'Temporary Internet Files' folder; and a vulnerability exists in the 'codebase' attribute of the 'object' tag due to a parsing error. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-014.mspx **An exploit script has been published.**	Microsoft Internet Explorer Vulnerabilities CAN-2005-0053 CAN-2005-0054 CAN-2005-0055 CAN-2005-0056	High	Microsoft Security Bulletin, MS05-014, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Notes VU#580299, VU#823971 VU#843771 VU#698835 **Security Focus, 12475, March 14, 2005**
PlatinumFTP PlatinumFTPserver 1.0.18	A remote Denial of Service vulnerability has been reported when a malicious user attempts to authenticate with a malformed user name. No workaround or patch available at time of publishing. An exploit script has been published.	PlatinumFTPServer Malformed User Name Connection Remote Denial of Service	Low	Security Focus 12790, March 12, 2005
PY Software Active WebCam 4.3, 5.5	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported when a malicious user submits a request for a file that exists on a floppy drive; a remote Denial of Service vulnerability has been reported when the 'Filelist.html' file is requested; an installation path disclosure vulnerability has been reported when a request is submitted for a non-existent file, which could let a remote malicious user obtain sensitive information; and an information disclosure vulnerability has been reported because different error messages are returned to a request for a file depending on whether the file exists or not, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PY Software Active Webcam Webserver Remote Denials of Service & Information Disclosure CAN-2005-0730 CAN-2005-0731 CAN-2005-0732 CAN-2005-0733 CAN-2005-0734	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA14553, March 10, 2005
SafeNet Sentinel License Manager 7.2.0.2	A buffer overflow vulnerability exists in the 'Lservnt' service on UDP port 5093 due to a boundary error, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. Upgrade to version 8.0 **An exploit script has been published.**	SafeNet Sentinel License Manager Remote Buffer Overflow CAN-2005-0353	High	CIRT.DK Advisory, March 7, 200 US-CERT VU#108790 **Security Focus, 12742, March 13, 2005**
Symantec AntiVirus Corporate Edition 9.0	A vulnerability has been reported when malicious files are placed on the server through an SMB share, which could bypass the detection mechanism. No workaround or patch available at time of publishing. There is no exploit code required.	Symantec AntiVirus SMB Scan Detection Bypass	Medium	Security Focus, 12808, March 15, 2005
Techland XPand Rally 1.0, 1.1	A format string vulnerability has been reported due to a failure of the application to securely call a formatted printing function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Techland XPand Rally Remote Format String CAN-2005-0729	High	Securiteam, March 10, 2005
Yahoo! Messenger 4.0, 5.0.1232, 5.0 .1065, 5.0 .1046, 5.0, 5.5.1249, 5.5, 5.6.0.1358, 5.6.0.1356, 5.6.0.1355, 5.6.0.1351, 5.6.0.1347, 5.6,	A buffer overflow vulnerability has been reported when a remote malicious user submits a custom message to a target buddy, which could lead to the execution of arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Yahoo! Messenger Custom Message Buffer Overflow CAN-2005-0737	High	Security Focus, 12750, March 8, 2005

6.0.0.1921, 6.0.0.1750, 6.0.0.1643, 6.0				

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Black List Daemon bld 0.3	A buffer overflow vulnerability has been reported due to the way the 'select()' system call is implemented, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. **Upgrade available at:** **http://www.online.redhate.org/bld/bld-0.3.2.tar.gz** An exploit has been published but has not been released to the public.	Black List Daemon select() Remote Buffer Overflow	Low/ High (High if arbitrary code can be executed)	Bugtraq, January 24, 2005 **Security Focus, 12347, March 11, 2005**
Frank McIngvale LuxMan 0.41 -17, 0.41	A buffer overflow vulnerability has been reported, which could let a malicious user execute arbitrary commands as ROOT. Debian: http://security.debian.org/pool/updates/main/l/luxman/luxman_0.41-17.2_i386.deb Currently we are not aware of any exploits for this vulnerability.	Frank McIngvale LuxMan Buffer Overflow CAN-2005-0385	High	Debian Security Advisory, DSA 693-1, March 14, 2005
Freeciv Freeciv 2.0 beta8	A remote Denial of Service vulnerability has been reported due to the way incomplete or modified requests are handled. No workaround or patch available at time of publishing. An exploit script has been published.	Freeciv Remote Denial of Service	Low	Security Focus, 12814, March 15, 2005
Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.suse.com/pub/suse/** FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CAN-2005-0064	High	iDEFENSE Security Advisory, January 18, 2005 Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005 Mandrakelinux Security Update Advisories, MDKSA-2005:016-021, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 Gentoo Linux Security Advisory, GLSA 200502-10, February 9, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 **SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005**

	Gentoo: http://security.gentoo.org/glsa/glsa-200502-10.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Trustix: http://http.trustix.org/pub/trustix/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ Currently we are not aware of any exploits for this vulnerability.			
GNU cpio 1.0, 1.1, 1.2	A vulnerability has been reported in 'cpio/main.c' due to a failure to create files securely, which could let a malicious user obtain sensitive information. Upgrades available at: http://ftp.gnu.org/gnu/cpio/cpio-2.6.tar.gz SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates** There is no exploit required.	CPIO Archiver Insecure File Creation CAN-1999-1572	Medium	Security Tracker Alert, 1013041, January 30, 2005 SGI Security Advisory, 20050204-01-U, March 7, 2005 **Turbolinux Security Advisory, TLSA-2005-30, March 10, 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161	GNU Xpdf Buffer Overflow in doImage() CAN-2004-1125	High	iDEFENSE Security Advisory 12.21.04 KDE Security Advisory, December 23, 2004 Mandrakesoft, MDKSA-2004:161,162,163,165,166, December 29, 2004 Fedora Update Notification, FEDORA-2004-585, January 6, 2005 Gentoo Linux Security Advisory, GLSA 200501-13, January 10, 2005 Conectiva Linux Security Announcement, CLA-2005:921, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Avaya Security Advisory, ASA-2005-027, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Fedora Legacy Update Advisory, FLSA:2353, February 10, 2005 Fedora Legacy Update Advisory, FLSA:2127, March 2, 2005 **SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005**

	Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166 Debian: http://www.debian.org/security/2004/dsa-619 Fedora (update for tetex): http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-13.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://support.sgi.com/browse_request/linux_patches_by_os Conectiva: ftp://atualizacoes.conectiva.com.br/ SuSE: ftp://ftp.suse.com/pub/suse/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			
Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CAN-2005-0706	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005
Hewlett Packard Company Tru64 4.0 G PK4, 4.0 F PK8, 5.1 B-2 PK4, 5.1 B-1 PK3, 5.1 A PK6	A Denial of Service vulnerability has been reported in the systems message queue. Patches available at: http://www.itrc.hp.com/service/patch/ Currently we are not aware of any exploits for this vulnerability.	HP Tru64 Message Queue Denial of Service CAN-2005-0719	Low	HP Security Bulletin, HPSBTU01109, March 9, 2005
Hiroyuki Yamamoto Sylpheed 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0.0-1.0.2	A buffer overflow vulnerability exists in certain headers that contain non-ASCII characters, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.3.tar.gz **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	Sylpheed Mail Client Remote Buffer Overflow CAN-2005-0667	High	Security Tracker Alert, 1013376, March 4, 2005 **Fedora Update Notification, FEDORA-2005-211, March 15, 2005**

ISC DHCPD 2.0.pl5	A format string vulnerability has been reported because user-supplied data is logged in an unsafe fashion, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://security.debian.org/pool/updates/main/d/dhcp/ We are not aware of any exploits for this vulnerability.	ISC DHCPD Package Remote Format String CAN-2004-1006	High	Debian Security Advisory, DSA 584-1, November 4, 2004 **US-CERT VU#448384**
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-17.xml** Currently we are not aware of any exploits for this vulnerability.	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications, FEDORA-2005-199 & 200, March 8, 2005 **Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005**
Marc Lehmann rxvt-unicode prior to 5.3	A buffer overflow vulnerability has been reported in 'command.c,' which could let a remote malicious user execute arbitrary code. Update available at: http://dist.schmorp.de/rxvt-unicode/rxvt-unicode-5.3.tar.bz2 Currently we are not aware of any exploits for this vulnerability.	Marc Lehmann rxvt-unicode 'command.c' Remote Buffer Overflow	High	Secunia Advisory: SA14562, March 15, 2005
Michael Kohn Ringtone Tools 2.22	A vulnerability was reported in Ringtone Tools. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted eMelody file that, when processed by the target user with Ringtone Tools, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the parse_emelody() function in 'parse_emelody.c.' **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-18.xml** A Proof of Concept exploit script has been published.	Michael Kohn Ringtone Tools parse_emelody() Buffer Overflow CAN-2004-1292	High	Security Tracker Alert ID, 1012573, December 16, 2004 **Gentoo Linux Security Advisory, GLSA 200503-18, March 15, 2005**
Multiple Vendors Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, rc1-rc3; libdbi-perl libdbi-perl 1.21, 1.42	A vulnerability exists libdbi-perl due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/libd/libdbi-perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-069.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libd/libdbi-perl/ Mandrake: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:030 SUSE: ftp://ftp.suse.com/pub/suse/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-38.xml** There is no exploit code required.	Libdbi-perl Insecure Temporary File Creation CAN-2005-0077	Medium	Debian Security Advisory, DSA 658-1, January 25, 2005 Ubuntu Security Notice, USN-70-1, January 25, 2005 Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005 RedHat Security Advisory, RHSA-2005:069-08, February 1, 2005 MandrakeSoft Security Advisory, MDKSA-2005:030, February 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 **Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005**

Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005
Multiple Vendors Perl	A race condition vulnerability was reported in the 'File::Path::rmtree()' function. A remote user may be able to obtain potentially sensitive information. A remote user may be able to obtain potentially sensitive information or modify files. The vendor has released Perl version 5.8.4-5 to address this vulnerability. Customers are advised to contact the vendor for information regarding update availability. Debian: http://security.debian.org/pool/updates/main/p/perl/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/perl-5.8.4-2.1.1.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Mandrake: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:031 SUSE: ftp://ftp.suse.com/pub/suse/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200501-38.xml** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability CAN-2004-0452	Medium	Ubuntu Security Notice, USN-44-1, December 21, 2004 Debian Security Advisory, DSA 620-1, December 30, 2004 OpenPKG Security Advisory, OpenPKG-SA-2005.001, January 11, 2005 Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005 MandrakeSoft Security Advisory, MDKSA-2005:031, February 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 **Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005**
Multiple Vendors IPsec-Tools IPsec-Tools 0.5; KAME Racoon prior to 20050307	A remote Denial of Service vulnerability has been reported when parsing ISAKMP headers. Upgrades available at: http://www.kame.net/snap-users/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service CAN-2005-0398	Low	Fedora Update Notifications, FEDORA-2005-216 & 217, March 14, 2005

Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1--test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **Ubuntu:** **http://security.ubuntu.com ubuntu/pool/main/l/linux-source-2.6.8.1/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/ Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005 Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005 **Ubuntu Security Notice, USN-95-1 March 15, 2005**
Multiple Vendors Linux kernel 2.6 .10, 2.6-2.6.11	Multiple vulnerabilities exist: a vulnerability exists in the 'radeon' driver due to a race condition, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the 'i2c-viapro' driver, which could let a malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'locks_read_proc()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in 'drivers/char/n_tty.c' due to a signedness error, which could let a malicious user obtain sensitive information; and potential errors exist in the 'atm_get_addr()' function and the 'reiserfs_copy_from_user_to_file_region()' function. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.11-rc4.bz2 SuSE: ftp://ftp.suse.com/pub/suse/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/** Exploit scripts have been published.	Linux Kernel Multiple Local Buffer Overflows & Information Disclosure **CAN-2005-0529** **CAN-2005-0530** **CAN-2005-0531** **CAN-2005-0532**	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14270, February 15, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005** **Ubuntu Security Notice, USN-95-1 March 15, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol) PPP Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ A Proof of Concept exploit script has been published.	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005
Multiple Vendors Sophos Sweep for Linux 3.91; Trend Micro Interscan Viruswall (Linux) 3.1	A vulnerability has been reported when processing a ZIP archive that contains malicious files with specially crafted file names, which could potentially allow malformed ZIP archives to bypass detection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept	Multiple Vendor Antivirus Products Malformed ZIP Archive Scan Evasion Bypass	Medium	Security Focus, 12793, March 12, 2005

	exploit has been published.			
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-15.xml** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 **Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005**
NewsScript.co.uk NewsScript	A vulnerability has been reported when a malicious user submits a specially crafted HTTP GET request, which could lead to unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required, however, a Proof of Concept exploit script has been published.	NewsScript Access Validation CAN-2005-0735	Medium	Security Focus, 12761, March 8, 2005
OpenBSD OpenBSD 2.0-2.9, 3.0-3.6	A remote Denial of Service vulnerability has been reported in the TCP timestamp processing functionality due to a failure to handle exceptional network data. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **An exploit script has been published.**	OpenBSD TCP Timestamp Remote Denial of Service CAN-2005-0740	Low	Security Tracker Alert, 1012861, January 12, 2005 **Security Focus, 12250, March 10, 2005**
OpenSLP OpenSLP 1.0.0-1.0.11, 1.1.5, 1.2 .0	Multiple buffer overflow vulnerabilities have been reported when processing malformed SLP (Service Location Protocol) packets, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=1730 SuSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for these vulnerabilities.	OpenSLP Multiple Buffer Overflows	High	SuSE Security Announcement, SUSE-SA:2005:015, March 14, 2005
PHP Arena paFileDB 3.1	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input before including in dynamically generated Web content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required, however, a Proof of Concept exploit has been published.	PaFileDB Multiple Cross-Site Scripting CAN-2005-0723	High	SecurityReason-2005-SRA#01, March 8, 2005
PHP Arena PaFileDB 3.1	An input validation vulnerability has been reported due to insufficient validation of the 'start' parameter in the '/includes/viewall.php' and '/includes/category.php' scripts, which could let a remote malicious user execute arbitrary SQL commands, HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PaFileDB 'viewall.php' and 'category.php' Input Validation CAN-2005-0724	High	SecurityReason-2005-SRA#03, March 12, 2005
PHP Arena PaFileDB prior to 3.1	A vulnerability has been reported in numerous scripts which could let a remote malicious user obtain the installation path. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PaFileDB Installation Path Disclosure	Medium	SecurityReason-2005-SRA#02, March 12, 2005
Rob Flynn Gaim 1.0-1.0.2, 1.1.1, 1.1.2	Multiple remote Denial of Service vulnerabilities have been reported when a remote malicious ICQ or AIM user submits certain malformed SNAC packets; and a vulnerability exists when parsing malformed HTML data. Upgrades available at:	Gaim Multiple Remote Denials of Service CAN-2005-0472	Low	Gaim Advisory, February 17, 2005 Fedora Update Notifications, FEDORA-2005-159 & 160, February 21, 2005

	http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-03.xml Mandrake: Http://www.mandrakesecure.net/en/advisories/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-215.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	CAN-2005-0473		US-CERT VU#839280 US-CERT VU#523888 Ubuntu Security Notice, USN-85-1 February 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-03, March 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005 **RedHat Security Advisory, RHSA-2005:215-11, March 10, 2005** **Conectiva Linux Security Announcement, CLA-2005:933, March 14, 2005**
Squid-cache.org Squid Web Proxy Cache 2.5 .STABLE5-STABLE8	A remote Denial of Service vulnerability has been reported when performing a Fully Qualify Domain Name (FQDN) lookup and and unexpected response is received. Patches available at: http://downloads.securityfocus.com/vulnerabilities/patches/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-25.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-173.html **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy FQDN Remote Denial of Service CAN-2005-0446	Low	Secunia Advisory, SA14271, February 14, 2005 Gentoo Linux Security Advisory GLSA, 200502-25, February 18, 2005 Ubuntu Security Notice, USN-84-1, February 21, 2005 Fedora Update Notifications, FEDORA-2005-153 & 154, February 21, 2005 SUSE Security Announcement, SUSE-SA:2005:008, February 21, 2005 Debian Security Advisory, DSA 688-1, February 23, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:047, February 24, 2005 RedHat Security Advisory, RHSA-2005:173-09, March 3, 2005 **Turbolinux Security Advisory, TLSA-2005-31, March 10, 2005**
SquirrelMail Development Team SquirrelMail 1.2.6	A vulnerability exists in 'src/webmail.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/squirrelmail 1.2.6-2_all.deb **Debian:** **http://security.debian.org/pool/updates/main/s/squirrelmail/** Currently we are not aware of any exploits for this vulnerability.	SquirrelMail Remote Code Execution CAN-2005-0152	High	Debian Security Advisory, DSA 662-1, February 1, 2005 US-CERT Vulnerability Note VU#203214 **Debian Security Advisory, DSA 662-2, March 14, 2005**

SquirrelMail S/MIME Plugin 0.4, 0.5	A vulnerability exists in the S/MIME plug-in due to insufficient sanitization of the 'exec()' function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.squirrelmail.org/plugin_view.php?id=54 **SUSE: ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	SquirrelMail S/MIME Plug-in Remote Command Execution CAN-2005-0239	High	iDEFENSE Security Advisory, February 7, 2005 US-CERT Vulnerability Note VU#502328 **SUSE Security Announcement, SUSE-SA:2005:015, March 14, 2005**
The PaX Team PaX linux 2.6.5, 2.4.20-2.4.28, 2.2.x	A vulnerability exists due to an undisclosed error, which could let a malicious user obtain elevated privileges and execute arbitrary code. Patches available at: http://pax.grsecurity.net/pax-linux-2.6.11-200503050030.patch **An exploit script has been published.**	PaX Undisclosed Arbitrary Code Execution CAN-2005-0666	High	Security Focus, 12729, March 4, 2005 **Security Focus, 12729, March 13, 2005**
Wine Windows API Emulator 20050310, 20050305, 20050211	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Wine Insecure File Creation	Medium	Security Focus, 12791, March 12, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
All Enthusiast PhotoPost PHP Pro version 5.0 RC3 up to but not including 5.0.1	Multiple vulnerabilities have been reported that could let remote malicious users conduct script insertion and SQL injection attacks, bypass certain security restrictions, and manipulate potentially sensitive information. These vulnerabilities are due to improper input validation in the "uid" parameter, "editbio" biography field and errors in the"adm-photo.php" script. The contents of uploaded images is also not properly verified. Upgrade to version 5.0.1. A Proof of Concept exploit has been published.	All Enthusiast PhotoPost PHP Pro Multiple Vulnerabilities	High	Security Focus, 12779, March 10, 2005
ApplyYourself i-Class	An access control vulnerability has been reported that could let a remote malicious user view sensitive information. A remote user can view a 7-digit ID value in the source code of their admission application and use that ID value to view unauthorized information. A fix is available at: applyyourself.com/products/products_iclass.asp A Proof of Concept exploit has been published.	ApplyYourself i-Class Information Disclosure Vulnerability CAN-2005-0747	Medium	Security Tracker Alert ID: 1013400, March 9, 2005
Bernd Ritter HolaCMS 1.4.9	An input validation vulnerability was reported in the Vote Module that could let a remote malicious user modify files on the target system. The 'vote_filename' parameter is not properly validated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Bernd Ritter HolaCMS Lets Remote Users Modify Files	High	Security Focus, 12799, March 14, 2005
Bösch SimpGB 1.x	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. This is due to input validation errors in the "quote" parameter in "guestbook.php" Update to version 1.35.2: http://www.boesch-it.de/sw/php-scripts/simpgb/english/download.php Currently we are not aware of any exploits for this vulnerability.	Bösch SimpGB "quote" SQL Injection Vulnerability	High	Security Focus, 12801, March 14, 2005
Cisco ACNS Software Version 4.2 and prior	Multiple vulnerabilities exist that could let remote users cause a Denial of Service. These are due to errors within the processing of TCP connections, IP packets, and network packets. he vulnerabilities affect devices configured as a transparent, forward, or reverse proxy server. A default password may also be available in the administrative account. Updates available: http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsdos.shtml Currently we are not aware of any exploits for these vulnerabilities.	Cisco ACNS Denial of Service Vulnerabilities CAN-2005-0601 CAN-2005-0600 CAN-2005-0599 CAN-2005-0598 CAN-2005-0597	Low	Cisco Security Advisory: 64069 Revision 1.0, February 24, 2005 **US-CERT VU#579240**
Computer Associates License 1.53 - 1.61.8	Multiple buffer overflow vulnerabilities exist that could let a remote malicious user execute arbitrary code with root level privileges. A remote user can also create files in arbitrary locations on the target system. This is because of input validation errors PUTOLF requests, GETCONFIG, and GCR requests. A fixed version (1.61.9) is available at: http://supportconnectw.ca.com/public/reglic/downloads/licensepatch.asp#alp **Another exploit script has been published.**	Computer Associates License Remote Code Execution Vulnerability CAN-2005-0581 CAN-2005-0582 CAN-2005-0583	High	iDEFENSE, 03.02.05 **Security Focus, 12705, March 10, 2005**

Ethereal Group Ethereal 0.10-0.10.8	A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code. **Upgrades available at:** **http://www.ethereal.com/download.html** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-16.xml** **Exploit scripts have been published.**	Ethereal Buffer Overflow CAN-2005-0699	High	Security Focus, 12759, March 8, 2005 **Security Focus, 12759, March 14, 2005** **Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005**
Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml A Denial of Service Proof of Concept exploit script has been published.	Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities CAN-2005-0704 CAN-2005-0705 CAN-2005-0739	Low/ HIgh (High if arbitrary code can be executed)	Ethereal Advisory, enpa-sa-00018, March 12, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005
GNU Gaim prior to 1.1.4	A vulnerability exists in the processing of HTML that could let a remote malicious user crash the Gaim client. This is due to a NULL pointer dereference. Update to version 1.1.4: http://gaim.sourceforge.net/downloads.php Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-85-1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-03.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-215.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	GNU Gaim Denial of Service Vulnerability CAN-2005-0208	Low	Sourceforge.net Gaim Vulnerability Note, February 24, 2005 US-CERT VU#795812 Gentoo, GLSA 200503-03, March 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005 **RedHat Security Advisory, RHSA-2005:215-11, March 10, 2005** **Conectiva Linux Security Announcement, CLA-2005:933, March 14, 2005**
GNU WF-Sections 1.07	A vulnerability has been reported that could let a remote malicious user inject SQL commands. This is due to input validation errors in the 'class/wfsfiles.php' script in the 'articleid' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU WF-Sections Input Validation Vulnerability CAN-2005-0725	High	Security Tracker Alert ID: 1013412, March 11, 2005
GNU Xoops 2.0.9.2	A vulnerability has been reported that could let a remote malicious user execute malicious scripts. This is due to an input validation error in the uploading of custom avatars in "uploader.php". Turn off support for custom avatar uploads in: System Admin -> Preferences -> User Info Settings -> "Allow	GNU Xoops Avatar Upload File Extension Vulnerability CAN-2005-0743	High	Xoops Security Bulletin, March 8, 2005

	Custom Avatar Upload" Patches available: http://www.xoops.org/modules/news/article.php?storyid=2114 Currently we are not aware of any exploits for this vulnerability.			
GNU YaBB2 RC1	An input validation vulnerability has been reported in 'usersrecentposts' that could let a remote malicious user conduct Cross-Site Scripting attacks. This is due to input validation errors in the 'usersrecentposts' action. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU YaBB Cross-Site Scripting Vulnerability CAN-2005-0741	High	Security Focus, Bugtraq ID 12756, March 15, 2005
Hensel Hartmann VoteBox 2.0	An include file vulnerability has been reported that could let a remote malicious user execute arbitrary commands on the target system. The 'votebox.php' script includes the 'votescontroller.php' script relative to the 'VoteBoxPath' variable and does not properly validate the user-supplied variable. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Hensel Hartmann VoteBox Arbitrary Code Execution Vulnerability	High	Systemsecure.org, Ref: SS#27022005, March 14, 2005
Hitachi Cosminexus Server Component Container and Cosminexus Server Component Container for Java	A vulnerability has been reported that could let a remote malicious user cause a Denial of Service. Vendor solutions available: http://www.hitachi-support.com/security_e/vuls_e/HS05-006_e/01-e.html Currently we are not aware of any exploits for this vulnerability.	Hitachi Cosminexus Server Component Container Tomcat Denial of Service	Low	Hitachi Advisory HS05-006, March 14, 2005 US-CERT VU#204710
IBM WebSphere Commerce 5.5, 5.6, and 5.6.0.1	A security issue has been reported that could disclose sensitive information. This is because the cache entry for a product or category display page can become linked to a prepopulated form, which may disclose private information. Apply fix pack 5.6.0.2 or later: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg21173312 Contact IBM product support to obtain APAR IY60949 for systems running WebSphere Commerce 5.5. Currently we are not aware of any exploits for this vulnerability.	IBM WebSphere Commerce Private Information Disclosure	Medium	IBM Security Advisory Reference #: 1199839, March 4, 2005
Infopop UBB.threads 6.x	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. This is due to an input validation error in the "Number" parameter in "editpost.php" Update to version 6.5.1.1. Currently we are not aware of any exploits for this vulnerability.	Infopop UBB.threads "Number" SQL Injection Vulnerability CAN-2005-0726	High	Secunia SA14578, March 14, 2005
Jason Hines phpWebLog 0.5.3	An include file vulnerability has been reported that could let a remote malicious user execute arbitrary commands on the target system. This is because of input validation errors in the 'include/init.inc.php' script in the 'G_PATH' parameter. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Jason Hines phpWebLog Arbitrary Commands Execution Vulnerability CAN-2005-0698	High	Security Tracker Alert ID: 1013397 Date: Mar 8 2005
Mozilla Thunderbird 1.0	A spoofing vulnerability has been reported that could let a remote malicious user create HTML that could spoof the status bar. This is caused due to an error embedding a table within an A HREF tag. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Thunderbird Status Bar Spoofing Vulnerability	Low	Secunia SA14567, March 14, 2005
Mozilla Firefox 1.0.1	A spoofing vulnerability has been reported that could let a remote malicious user create HTML that could spoof the status bar. This is caused due to an error embedding a table within an A HREF tag. No workaround or patch available at time of publishing.	Mozilla Firefox Status Bar Spoofing Vulnerability	Low	Security Tracker Alert ID: 1013423, March 14, 2005

	A Proof of Concept exploit has been published.			
Mozilla Mozilla 1.7.5	A spoofing vulnerability has been reported that could let a remote malicious user create HTML that could spoof the status bar. This is caused due to an error embedding a table within an A HREF tag. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Status Bar Spoofing Vulnerability	Low	Secunia SA14568, March 14, 2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability has been reported that could let local malicious users gain escalated privileges. This is because the "CREATE TEMPORARY TABLE" command can create insecure temporary files. The vulnerabilities have been fixed in version 4.0.24 (when available): http://dev.mysql.com/downloads/ A Proof of Concept exploit has been published.	MySQL Escalated Privilege Vulnerabilities CAN-2005-0711	Medium	Secunia SA14547, March 11, 2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/ downloads/index.html A Proof of Concept exploit has been published.	MySQL CREATE FUNCTION Remote Code Execution Vulnerability CAN-2005-0709	High	Security Tracker Alert ID: 1013415, March 11, 2005
MySQL AB MySQL 4.0.23, and 4.1.10 and prior	An input validation vulnerability was reported in udf_init() that could let an authenticated user with certain privileges execute arbitrary library functions on the target system. The udf_init() function in 'sql_udf.cc' does not properly validate directory names. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/ downloads/index.html A Proof of Concept exploit has been published.	MySQL udf_init() Path Validation Vulnerability CAN-2005-0710	High	Security Tracker Alert ID: 1013414, March 11, 2005
MySQL MaxDB Web Agent prior to 7.5.00.24	Several vulnerabilities have been reported that could let a remote user conduct Denial of Service attacks. This is due to input validation errors in multiple functions. A fixed version (7.5.00.24) is available at: http://dev.mysql.com/ downloads/maxdb/7.5.00.html No workaround or patch available at time of publishing.	MaxDB Web Agent Denial of Service Vulnerability CAN-2005-0083	High	iDEFENSE Security Advisory 03.14.05
Nick Jones PHP-Fusion 5.x	A vulnerability has been reported that could let remote malicious users conduct script insertion attacks. This is due to input validation errors in HTML encoded input (e.g. &#[ASCII]) passed in BBcode. Updates available in the CVS repository. An exploit script has been published.	Nick Jones PHP-Fusion Script Insertion Vulnerability CAN-2005-0692	High	Secunia SA14492, March 8, 2005
Novell Novell iChain 2.x	A vulnerability has been reported that could let a remote malicious user gain knowledge of certain system information. This is due to an error in the FTP server that allows "PWD" commands to be executed prior to user authentication. Restrict access to the iChain server. Currently we are not aware of any exploits for this vulnerability.	Novell iChain FTP Server Path Disclosure Weakness CAN-2005-0746	Medium	Novell, Technical Information Document ID: 10096886, March 8, 2005
Novell Novell iChain 2.x	A vulnerability has been reported that could let a remote malicious user bypass the user authentication. This is because of an error in the web GUI that permits the user to hijack an administrator's session. Restrict access to the iChain server via the web GUI (port 51100/tcp). Currently we are not aware of any exploits for this vulnerability.	Novell iChain Administrator Session Hijacking Vulnerability CAN-2005-0744	Medium	Novell, Technical Information Document ID: 10096885, March 8, 2005

OutStart Participate Enterprise	Multiple vulnerabilities have been reported that could let a remote malicious user view directories and rename or delete directory objects. The vendor has issued a fix. A Proof of Concept exploit has been published.	OutStart Participate Enterprise Multiple Vulnerabilities CAN-2005-0685	Medium	Outstart Security Notification, March 8, 2005
phorum.org Phorum 5.0.14	Several input validation vulnerabilities were reported in Phorum in 'file.php,' 'follow.php,' and the user's control panel that could let a remote malicious user conduct Cross-Site Scripting attacks. Update to version 5.0.15: http://sourceforge.net/project/showfiles.php?group_id=107 Currently we are not aware of any exploits for these vulnerabilities.	Phorum Input Validation Vulnerabilities	High	Secunia SA14554, March 11, 2005 Security Tracker Alert ID: 1013422, March 14 2005
phpAdsNew phpAdsNew 2.0.4 -pr1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPAdsNew AdFrame.PHP Cross-Site Scripting	High	Security Focus, 12803, March 14, 2005
phpAdsNew phpAdsNew 2.x and phpPgAds 2.x	A vulnerability has been reported that could let remote malicious users conduct Cross-Site Scripting attacks or view sensitive information. This is because of input validation errors in the "refresh" parameter in "adframe.php". Update to phpPgAds 2.0.4-pr2: http://sourceforge.net/project/showfiles.php?group_id=36679 Update to phpAdsNew 2.0.4-pr2: http://sourceforge.net/project/showfiles.php?group_id=11386 Currently we are not aware of any exploits for this vulnerability.	phpPgAds / phpAdsNew "refresh" Cross-Site Scripting Vulnerability	High	Secunia SA14592, March 15, 2005
PHP Arena paBox 2.0	A vulnerability has been reported in 'pabox.php' due to insufficient sanitization of the 'posticon' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PABox 'Posticon' Arbitrary HTML Execution	High	Secunia Advisory, SA14590, March 15, 2005
phpBB Group phpBB 2.0.13 and prior	A vulnerability exists in 'oracle.php' that could let a remote user determine the installation path. A remote user can access 'phpBB/db/oracle.php'. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	phpBB Group phpBB 'oracle.php' Information Disclosure **CAN-2005-0659** **(CVE number corrected)**	Low	[N]eo [S]ecurity [T]eam [NST] - Advisory #09 - 03/03/05
phpforums.net mcNews 1.3	An include file vulnerability has been reported that could let a remote malicious user execute arbitrary commands on the target system. This is because of input validation errors in the 'mcNews/admin/header.php' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	phpforums.net mcNews Code Execution Vulnerability CAN-2005-0720	High	Security Tracker Alert ID: 1013396 Date: Mar 8 2005
Radek Hulan BLOG:CMS 3.6.2	A vulnerability exists that could let remote malicious users conduct SQL injection attacks. Update to version 3.6.2 or later: http://blogcms.com/?item=download Currently we are not aware of any exploits for this vulnerability.	Radek Hulan BLOG:CMS PunBB SQL Injection Vulnerabilities CAN-2005-0569	High	Secunia SA14538, March 9, 2005
RealNetworks RealPlayer prior to 6.0.12.1059	A vulnerability in the processing of SMIL files could let a remote malicious user execute arbitrary code. A special Synchronized Multimedia Integration Language (smil) file could trigger to trigger a buffer overflow in the player's SMIL parser. The vulnerability is in 'datatype/smil/renderer/smil1/smlparse.cpp' when processing the screen size attribute. Updates available at: http://service.real.com/help/faq/	RealNetworks RealPlayer SMIL Error Permits Remote Code Execution CAN-2005-0455	High	iDEFENSE Security Advisory 03.01.05 **SUSE-SA:2005:014, March 9, 2005**

	security/050224_player/EN/ **SUSE:** **ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/RealPlayer-10.0.3-0.1.i586.rpmcf95cd77f9abda58abff3b488c55a515** **Proof of Concept exploit script has been published.**			
RealNetworks RealPlayer prior to 6.0.12.1059	A vulnerability in the processing of WAV files could let a remote malicious user execute arbitrary code. A special WAV file could trigger a buffer overflow and execute arbitrary code. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/ **SUSE:** **ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/RealPlayer-10.0.3-0.1.i586.rpmcf95cd77f9abda58abff3 b488c55a515** Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer WAV File Error Permits Remote Code Execution CAN-2005-0611	High	RealPlayer Release Notes March 1, 2005 **SUSE-SA:2005:014, March 9, 2005**
Smarter Scripts The Includer	A vulnerability exists that could let a remote malicious user execute arbitrary commands on the target system. This is due to input validation errors in the 'includer.cgi' script. No workaround or patch available at time of publishing. **An exploit script has been published.**	Smarter Scripts The Includer Remote Code Execution Vulnerability CAN-2005-0689	High	Security Focus, Bugtraq ID 12738, March 7, 2005 **Security Focus, Bugtraq ID 12, 2005**
SocialMPN SocialMPN 1.2.1-1.2.5	A vulnerability has been reported in the article mode for 'modules.php' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://socialmpn.com/download.php?op=getit&lid=20 An exploit script has been published.	SocialMPN 'modules.php' Arbitrary Code Execution CAN-2005-0691	High	Security Focus, 12774, March 10, 2005
Spinworks.net Spinworks Application Server 3.0	A remote Denial of Service vulnerability has been reported due to a failure to properly handle malformed requests. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Spinworks Application Server Remote Denial of Service	Low	Secunia Advisory, SA14579, March 14, 2005

SquirrelMail Development Team SquirrelMail 1.x	A Cross-Site Scripting vulnerability exists in the 'decodeHeader()' function in 'mime.php' when processing encoded text in headers due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://prdownloads.sourceforge.net/squirrelmail/sm143a-xss.diff?download Gentoo: http://security.gentoo.org/glsa/glsa-200411-25.xml Conectiva: ftp://atualizacoes.conectiva.com.br/9 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Apple: http://www.apple.com/support/downloads/ SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://www.debian.org/security/2005/dsa-662 Red Hat: http://rhn.redhat.com/errata/RHSA-2005-135.html **Debian:** **http://security.debian.org/pool/updates/main/s/squirrelmail/** An exploit script is not required.	SquirrelMail Cross-Site Scripting CAN-2004-1036 CAN-2005-0104 CAN-2005-0152	High	Secunia Advisory, SA13155, November 11, 2004 Gentoo Linux Security Advisory, GLSA 200411-25, November 17, 2004 Fedora Update Notifications, FEDORA-2004-471 & 472, November 28, 2004 Conectiva Linux Security Announcement, CLA-2004:905, December 2, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 Debian DSA-662-1, February 1, 2005 Red Hat RHSA-2005:135-04, February 10, 2005 **Debian Security Advisory, DSA 662-2, March 14, 2005**
Sun Microsystems, Inc. Sun Java System Application Server 7.0 UR5 Standard Edition, Platform Edition, 7.0 UR4, 7.0 2004Q2 R1Standard, 7.0 2004Q2 R1Enterprise, 7.0 Standard Edition, 7.0 Platform Edition, 7.0 2004Q2	A Cross-Site Scripting vulnerability has been reported, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-577421&searchclause=%22category:security%22%20%22availability,%20security%22 There is no exploit code required.	Sun Java System Application Server Unspecified Cross-Site Scripting CAN-2005-0742	High	Sun(sm) Alert Notification, 57742, March 1, 2005
UTStarcom iAN-02EX VoIP ATA	A security issue exists that could let a local malicious user bypass certain security restrictions. This is because the ATA (Analog Terminal Adaptor) can be reset by dialing "*#26845#". No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	UTStarcom iAN-02EX VoIP ATA Reset Security Bypass CAN-2005-0745	Medium	Secunia SA14544, March 9, 2005
WEBInsta Mailing list manager 1.3d	A vulnerability has been reported that could let a remote malicious user include arbitrary files from external and local resources. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	WEBInsta Mailing list manager Arbitrary File Inclusion Vulnerability CAN-2005-0748	High	Secunia SA14550, March 10, 2005
Xerox Document Centre 535/545/555 (27.18.017 or prior), 460/470/480/490 (19.01.037 - 19.05.521 and 19.5.902 - 19.5.912), 420/426/432/440 (with ESS 2.1.2 - 3.21), 425/432/440 (with ESS	A vulnerability has been reported that can let local malicious users bypass certain security restrictions. This is due to an unspecified error in the web server on the ESS/ Network Controller Update: http://www.xerox.com/downloads/usa/en/c/cert_P16_DCAccess_Patch.zip Currently we are not aware of any exploits for this vulnerability.	Xerox Document Centre Web Server Unauthorized Access Vulnerability	Medium	XEROX SECURITY BULLETIN XRX05-003, March 7, 2005

3.0.5.4 - 3.2.30), 430 (with ESS 3.3.23 - 3.3.30), 240/255/265 (18.01 - 18.6.81)				
Xerox Document Centre 535/545/555 (27.18.017 or prior). 460/470/480/490 (versions 19.01.037 - 19.05.521 and 19.5.902 - 19.5.912), 420/426/432/440 (with ESS 2.1.2 - 2.3.21), 425/432/440 (with ESS 3.0.5.4 - 3.2.30), 430 (with ESS 3.3.24 - 3.3.30)	A vulnerability has been reported that could let malicious users cause a Denial of Service. This is due to an unspecified memory corruption error in the MicroServer Web Server when processing URLs. Update: http://www.xerox.com/downloads/usa/en/c/cert_P11_DCMemory_Patch.zip Currently we are not aware of any exploits for this vulnerability.	Xerox MicroServer Web Server URL Handling Denial of Service	Low	XEROX SECURITY BULLETIN XRX05-004, March 7, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
March 15, 2005	3com_3cdaemon_ftp_overflow.pm	No	Script that exploits the 3Com 3CDaemon Multiple Remote Vulnerabilities.
March 15, 2005	covertsession-0.4.c	N/A	A command line tool that allows you to create a TCP session that IDS sensors cannot parse correctly.
March 15, 2005	exp2.php.txt	Yes	Proof of Concept exploit for the MySQL CREATE FUNCTION Remote Code Execution Vulnerability.
March 15, 2005	exp3.pl.txt	Yes	Proof of Concept exploit for the libc MYSQL User Privilege vulnerability.
March 15, 2005	freeciv.pl	No	Perl script that exploits the Freeciv Remote Denial of Service vulnerability.
March 15, 2005	goodTechTelnetBufferOverflowPoC.c	No	Proof of Concept exploit for the GoodTech Systems Telnet Server for Windows NT/2000/XP/2003 Remote Buffer Overflow vulnerability.
March 15, 2005	kernel26lowmem.txt	No	Sample exploitation for the Linux Kernel SYS_EPoll_Wait Elevated Privilege vulnerability.
March 15, 2005	ms04038.c	Yes	Exploit for Internet Explorer (mshtml.dll) that makes use of a buffer overflow when parsing Cascading Style Sheets (CSS) files.
March 15, 2005	plsql_portscanner-0.1.tar.gz	N/A	A TCP CONNECT port scanner in P/L SQL code.
March 15, 2005	real-seh.cpp	Yes	Proof of Concept exploit for the RealNetworks RealPlayer SMIL Error Permits Remote Code Execution vulnerability.
March 15, 2005	silePNEWSxpl_v2.0b4.c	Yes	Exploit for the paNews version 2.0b4 SQL injection vulnerability.
March 14, 2005	ethereal-0.10.10.tar.gz	N/A	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
March 14, 2005	ethereal3GA11OverflowExploit.c ethereal-g3-a11.c eth0day.c	Yes	Exploits for the Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities.
March 14, 2005	IEDragAndDropExploit.zip	Yes	Exploit for the Microsoft Internet Explorer Vulnerabilities.
March 13, 2005	101_SentLM.cpp	Yes	Exploit for the SafeNet Sentinel License Manager Remote Buffer Overflow vulnerability.
March 13, 2005	paxomatic.c	Yes	Exploit for the PaX Undisclosed Arbitrary Code Execution vulnerability.
March 12, 2005	aztec-sploit.c	No	Proof of Concept exploit for the Aztek Forum Unauthorized Access Vulnerability.
March 12, 2005	etherealIAPPOverflow-poc.cIAPPOverflow-poc.c	Yes	Denial of Service Proof of Concept exploit for the Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities.
March 12, 2005	includer.py	No	Exploit for the Smarter Scripts The Includer Remote Code Execution Vulnerability.
March 12, 2005	pftpdos1.pl	No	Perl script that exploits the PlatinumFTPServer Malformed User Name Connection Remote Denial of Service vulnerability.
March 12, 2005	phpBB2012session.txt	Yes	Exploit for the phpBB 2.0.12 session handling administrative compromise vulnerability.

March 12, 2005	phpFM.py.txt	No	Exploit for the Stadtaus.Com PHP Form Mail Script Remote File Include vulnerability.
March 12, 2005	phpfusionXSS.txt	Yes	Detailed exploitation for the Nick Jones PHP-Fusion Script Insertion Vulnerability.
March 12, 2005	windos.c	No	Exploit for the Windows Server 2003 and XP SP2 Remote Denial of Service vulnerability.
March 11, 2005	exp2.php exp3.pl	Yes	Exploits for the MySQL AB MySQL Multiple Remote Vulnerabilities.
March 11, 2005	happy-crc.zip	No	Proof of Concept exploit for the Multiple Vendor Antiviral Products Malformed ZIP Attachment Scan Evasion Vulnerability.
March 10, 2005	CALicenseBOExplClass101.cpp 101_cali.c	Yes	Exploit for the Computer Associates License Remote Code Execution Vulnerability.
March 10, 2005	r57obsd-dos.c obsdDoS.c	Yes	Exploits for the OpenBSD TCP Timestamp Remote Denial of Service vulnerability.
March 9, 2005	socialmpn_exploit.pl socialMPN.txt	Yes	Perl script that exploits the SocialMPN 'modules.php' Arbitrary Code Execution vulnerability.
March 9, 2005	xprallyfs.zip	No	Exploit for the Techland XPand Rally Remote Format String Vulnerability.
March 8, 2005	ie_css_bof.c	No	Exploit for the Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote Buffer Overflow vulnerability.

[back to top]

Trends

- According to a study from The Honeynet Project, botnets launched 226 distributed denial of service (DDoS) attacks on 99 different targets in a three-month period from November 2004 to January 2005. The report, Know your Enemy: Tracking Botnets, estimates a population of approximately one million infected hosts is under the control of computer crackers. For more information, see "Rise of the botnets" located at: http://www.theregister.co.uk/2005/03/15/honeypot_botnet_study/
- The Internet Storm Center (ISC) tracked a large-scale hack over the weekend that infected site-hosting servers, which in turn transformed all the hosted sites into distributors of malicious code. For more information, see "Weekend Attack Infects Hosting Servers ' located at: http://www.securitypipeline.com/news/159402903
- Analytical findings published by iDefense, a Reston, Va.-based supplier of security intelligence to both corporations and government agencies, were made public for the first time. Using their private database of more than 100,000 malicious code attacks, iDefense tallied a record 27,260 attacks in 2004. Over 15,000 of those, or some 55 percent, were specifically designed to covertly steal information or take over computers for criminal purposes, including identify theft and fraud. Over 9,000 backdoors dropped by most mass-mailed worms were counted. For more information, see " Root of all evil is root of most attacks" located at: http://www.internetweek.com/showArticle.jhtml?articleID=159400994
- Security consultants have uncovered a device, BlueSniper, that can pick up transmissions on Bluetooth modules up to 1km away.The device consists of a directional 'yagi' antenna mounted on a foldable stock with a Bluetooth module and processor built into the magazine, although it can also be hooked up to a laptop. For more information, see "Hackers target Bluetooth devices 1km away" located at: http://www.vnunet.com/news/1161915

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Slight Increase	March 2004
2	Bagle-BJ	Win32 Worm	Slight Decrease	January 2005
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
8	Netsky-B	Win32 Worm	Stable	February 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Bagle.BB	Win32 Worm	Stable	September 2004

Table Updated March 15, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Bagle, Zafi and Netsky coders thought to be working together: The authors of the Bagle, Zafi and Netsky viruses have joined forces in an unholy alliance that aims to spread cyber-terror, security experts have claimed. The warning comes from virus analysts at Kaspersky Lab investigating the recent Bagle outbreak and suggest that the authors of Bagle, Zafi and Netsky are "working hand in hand with each other". For more information, see: http://www.vnunet.com/news/1161786

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Haiyangweng		Trojan
Backdoor.Ranky.T		Trojan
Backdoor.Solufina		Trojan
Backdoor.Staprew		Trojan
Backdoor.Zins.B		Trojan
BKDR_SDBOT.LG		Trojan
Openstream.T	Java/Openstream.T	Trojan
PE_ZORI.A	Virus.Win32.Zori.a W32.Zori.A W32/Generic.Delphi	Win32 Worm
PWSteal.Reanet.B		Trojan
Ruzes.A	Trj/Ruzes.A	Trojan
Troj/Dowcen-Gen		Trojan
Trojan.Adwarehelper		Trojan
Trojan.Adwareloader		Trojan
Trojan.Flush.B		Trojan
Trojan.Kaemon		Trojan
Trojan.Lodmedud		Trojan
Trojan.StartPage.K		Trojan
Trojan.StartPage.L		Trojan
Trojan.StartPage.M		Trojan
Trojan.Tabela.B		Trojan
W32.Kelvir.E		Win32 Worm
W32.Kelvir.G		Win32 Worm
W32.Kelvir.H		Win32 Worm
W32.Mytob.E@mm		Win32 Worm
W32.Mytob.F@mm	Net-Worm.Win32.Mytob.d W32.Mytob.E@mm W32/Mytob.gen@MM Win32.Mytob.F Win32/Mytob.D@mm WORM_MYTOB.F	Win32 Worm
W32.Mytob.G@mm	Net-Worm.Win32.Mytob.d	Win32 Worm
W32.Selotima.A		Win32 Worm
W32.Serflog.C		Win32 Worm
W32.Toxbot		Win32 Worm
W32/Agobot-QT	Win32.Agobot.xs W32/Agobot.CVS	Win32 Worm
W32/Agobot-QU	Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Agobot-QV	Backdoor.Win32.Agobot.gen W32/Gaobot.worm.gen.d	Win32 Worm
W32/Agobot-QX		Win32 Worm
W32/Capside-C	WORM_CASPID.C Win32/Capside.C P2P-Worm.Win32.Capside.c	Win32 Worm
W32/Domwis-H	BKDR_DOMWIS.C Backdoor.Win32.Wisdoor.av	Win32 Worm
W32/Elitper-C	WORM_ELITPER.C	Win32 Worm
W32/Esalone-A	Trojan.Win32.Delf.ir W32/Eightsalone.worm	Win32 Worm
W32/Myfip.worm.q	W32.Myfip.T	Win32 Worm
W32/Radbot-A		Win32 Worm
W32/Radebot.worm		Win32 Worm

W32/Rbot-XE		Win32 Worm
W32/Rbot-XI	W32/Sdbot.worm.gen.h WORM_RBOT.ASU	Win32 Worm
W32/Rbot-XM	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-XS	Backdoor.Win32.SdBot.lt	Win32 Worm
W32/Sdbot.gen.r		Win32 Worm
W32/Sdbot.worm!48548		Win32 Worm
W32/Sdbot-VW	W32/Sdbot.worm.gen Backdoor.Win32.SdBot.gen WORM_RBOT.AJS	Win32 Worm
W32/Sumom-B	WORM_FATSO.B IM-Worm.Win32.Sumom.a	Win32 Worm
Win32.Agobot.AQW		Win32 Worm
Win32.Bropia.T		Win32 Worm
Win32.Mytob.B		Win32 Worm
Win32.Mytob.C		Win32 Worm
Win32.Mytob.D		Win32 Worm
Win32.Podilk.A		Win32 Worm
WORM_CHOD.A	Backdoor.Win32.VB.aam Tobecho.A W32.Chod@mm W32/NoChod@MM W32/Tobecho.A.worm Win32.Nochod.A Worm:Win32/Chod.A	Win32 Worm
WORM_CODBOT.L	MS03-026_Exploit!Trojan W32.Toxbot Worm:Win32/Codbot.L	Trojan
WORM_ELITPER.C		Win32 Worm
WORM_ELITPER.D	W32.Elitper.D@mm W32/Elitper-D W32/Generic.m Win32.Elitper.B	Win32 Worm
WORM_FORBOT.AB	Backdoor:Win32/Wootbot.AG W32/Forbot-ET W32/Sdbot.worm Win32.ForBot.MY	Win32 Worm
WORM_KELVIR.D	W32/Bropia-G W32/Kelvir.worm Win32.Bropia.T	Win32 Worm
WORM_KELVIR.E	W32/Kelvir.worm	Win32 Worm
WORM_KELVIR.F	W32.Kelvir.F W32/Bropia-K W32/Bropia.worm Win32.Bropia.S	Win32 Worm
WORM_MYDOOM.BF	W32/Mydoom W32/MyDoom-J Win32.Mydoom.BH	Win32 Worm
WORM_MYFIP.M	W32/Myfip.worm	Win32 Worm

[back to top]

Last updated March 16, 2005